УДК 003.26.09; 519.688

[1]Юрій Кондрацький, [1]Андрій Луцків, [2]Юсуф Наботов
[1]Тернопільський національний технічний університет імені Івана Пулюя, Україна
[2]Технологічний університет Таджикистану, Таджикистан

ПРАКТИЧНІ АСПЕКТИ ЗДІЙСНЕННЯ КРИПТОАНАЛІЗУ МЕТОДОМ «СЕНДВІЧ АТАКИ З ПОВ'ЯЗАНИМИ КЛЮЧАМИ» АЛГОРИТМУ KASUMI

Yuriy Kondratskyy, Andriy Lutskiv

PRACTICAL ASPECTS OF KASUMI ALGORITHM CRYPTANALYSIS BY «SANDWICH ATTACK WITH RELATED KEYS»-METHOD

З розвитком та поширенням телекомунікаційних технологій постає задача забезпечення конфіденційності інформації. KASUMI – це блоковий шифр, який був спроектований Security Algorithms Group of Experts (SAGE). Він базується на мережі Фейстеля з 8 раундами і генерує 64-бітне вихідне значення з 64-бітного вхідного значення, використовуючи 128-бітний ключ [1].

На даний час найкращою відомою криптоаналітичною атакою на KASUMI є «Сендвіч атака з пов'язаними ключами» [2]. Даний метод розглядає шифр як структуру з трьох рівнів: перший рівень включає в себе перших 3 раунди, другий – 4-й раунд, третій – 5-7 раунди. В восьмому раунді використовується метод повного перебору для знаходження 32 біт ключа шифрування. Загалом атака на алгоритм шифрування KASUMI складається з етапів, які подані на рисунку 1.

Часова складність даного методу становить $2^{32,}$ і на сьогодні є найоптимальнішою за часом у порівнянні з попередніми, які становили 2^{76}[2]. Складність за даними «сандвіч атаки» становить 2^{26}, тобто 2^{25} обраних шифротекстів та 2^{25} адаптивно підібраних відкритих текстів, які зашифровані/розшифровані одним із чотирьох пов'язаних ключів. Складність пам'яті (просторова складність) даної атаки залежить від особливостей вхідних даних й може дещо відрізнятися для різних вхідних даних, проте наближене значення необхідного об'єму пам'яті становить 1,1 Gb. Зазначимо, що наведені значення визначають часову й просторову складності, а також складність за необхідними вхідними даними для одного набору вхідних даних. Таким чином, з метою зменшення часу здійснення криптоаналізу, доцільно здійснити декомпозицію обчислювальної задачі та реалізувати її з використання методів та засобів паралельних і розподілених обчислень.

Перший етап криптоаналітичної атаки полягає у плануванні пов'язаних ключів і не потребує великих обчислювальних ресурсів, тому не має необхідності разпаралелювати дану задачу.

На другому етапу генеруються 226 пар відкритих текстів та шифротекстів. Оскільки, генерація пар не є ресурсоємним процесом, тому доцільність розпаралелення відсутня.

Третій етап передбачає визначення та аналіз квартетів й вимагає значних обчислювальних ресурсів, тому для його оптимізації потрібно здійснити розпаралелення.

Четвертий етап полягає в повному переборі останніх 32 бітів ключа, що також є достатньо ресурсоємним процесом й доцільно здійснити його розпаралелення для зменшення часу виконання. Даний етап передбачає використання значних обчислювальних потужностей для одного набору вхідних даних, а при їх збільшенні — вимоги до обчислювальних потужностей, оперативної пам'яті та сховищ даних також будуть вищими.

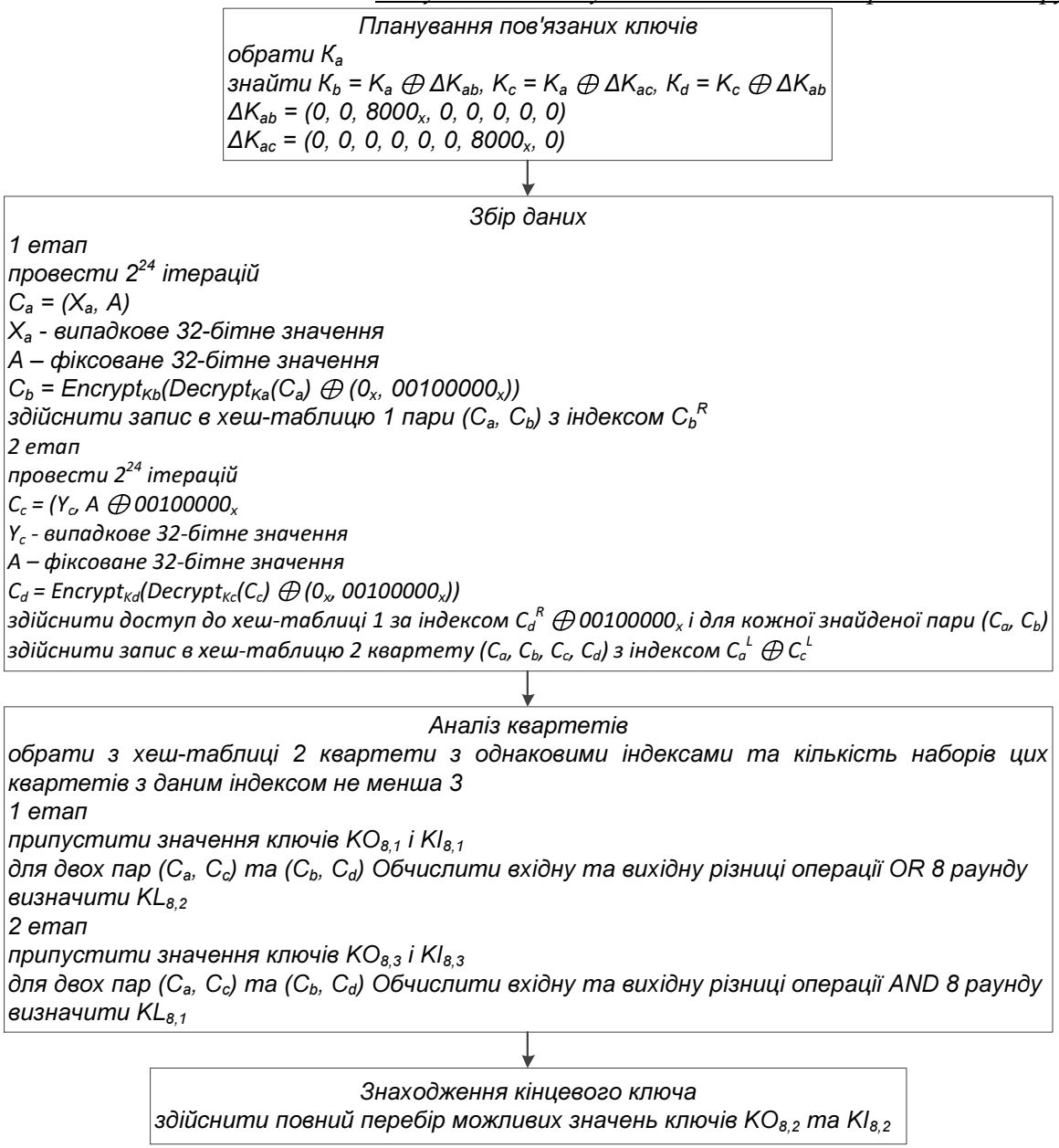

Рис. 1. Загальна схема криптоаналітичного алгоритму [2]

Для реалізації даного методу криптоаналізу в паралельних та розподілених обчислювальних системах реалізовано програмне забезпечення з використанням технологій розпаралелення — OpenMP та MPI

Література

1. 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".

2. Orr Dunkelman, Nathan Keller, Adi Shamir (2010-01-10). A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, Weizmann Institute of Science 10 January 2010 [Електронний ресурс]. – Режим доступу: URL: http://eprint.iacr.org/2010/013.pdf.